МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Царегородцев Кирилл Денисович

Правильные семейства функций и порождаемые ими квазигруппы: комбинаторные и алгебраические свойства

1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2025

Диссертация подготовлена на кафедре математической теории интеллектуальных систем механико-математического факультета МГУ имени М.В. Ломоносова.

Научные руководители: **Панкратьев Антон Евгеньевич,**
кандидат физико-математических наук

Галатенко Алексей Владимирович,
кандидат физико-математических наук

Официальные оппоненты: **Щучкин Николай Алексеевич,**
доктор физико-математических наук, доцент,
Волгоградский государственный социально-педагогический университет, Институт математики, информатики и физики, кафедра высшей математики и физики, профессор

Камловский Олег Витальевич,
доктор физико-математических наук, доцент,
МИРЭА — Российский технологический университет, Институт искусственного интеллекта, кафедра 252, профессор

Токарева Наталья Николаевна,
кандидат физико-математических наук,
Новосибирский национальный исследовательский государственный университет, механико-математический факультет, кафедра теоретической кибернетики, доцент

Защита диссертации состоится «21» ноября 2025 г. в 18 часов 45 минут на заседании диссертационного совета МГУ.011.4 Московского государственного университета имени М. В. Ломоносова по адресу: 119234, Москва, ГСП-1, Ленинские горы, д. 1, МГУ имени М.В. Ломоносова, механико-математический факультет, аудитория 14-08.

E-mail: dissovet.msu.011.4@math.msu.ru.

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М. В. Ломоносова (Ломоносовский просп., д. 27) и на портале https://dissovet.msu.ru/dissertation/3562/

Автореферат разослан «____» октября 2025 года.

Ученый секретарь
диссертационного совета МГУ.011.4,
кандидат физико-математических наук В. А. Кибкало

Общая характеристика работы

Актуальность темы.

Диссертация посвящена вопросам, лежащим на стыке дискретной математики (теория дискретных функций), алгебры (теория квазигрупп) и криптографии. Основным объектом изучения является особый класс дискретных функций, введенных В. А. Носовым[1] (т.н. «правильные семейства» функций), которые могут быть использованы для построения параметрических классов квазигрупп. Квазигруппы — одна из базовых структур в алгебре. Таблицы умножения квазигрупп, более известные под названием «латинские квадраты», с древнейших времен и по настоящее время используются в различных областях математики (см., например, монографию Й. Денеша и Э.Д. Кидвелла[2]): при планировании статистических экспериментов, в играх и головоломках, а также в теории кодирования и криптографии, которые рассматриваются более подробно в настоящей работе. Из общих обзоров криптографических приложений квазигрупп можно отметить следующие источники:

- статья М.М. Глухова[3], в которой приводятся примеры кодов аутентификации, шифров и однонаправленных функций на основе квазигрупповых преобразований, а также недавний обзор индийских авторов[4], затрагивающий тематику построения симметричных криптопримитивов на основе квазигрупповых операций;
- монография В. Щербакова[5], в которой довольно подробно освещена тематика использования квазигрупп в криптографии; в частности, в работе рассматриваются следующие темы: поточные шифры и их криптоанализ, хэш-функции и односторонние функции, схемы разделения секрета; а также смежная тематика теории кодирования (в частности, рекурсивные МДР-коды);
- монография Й. Денеша и Э.Д. Кидвелла[6] и статья М.Э. Тужилина[7], посвященные общим обзорам тематики латинских квадратов, их использованию в докомпьютерный этап развития криптографии и современным приложениям.

---

[1] *Носов В. А.* Критерий регулярности булевского неавтономного автомата с разделенным входом // Интеллектуальные системы. Теория и приложения. 1998. Т. 3, № 3/4. С. 269—280; *Носов В. А.* Построение классов латинских квадратов в булевой базе данных // Интеллектуальные системы. Теория и приложения. М., 1999. Т. 4, № 3/4. С. 307—320.

[2] *Denes J., Keedwell A.* Latin squares and their applications (2nd edition). Elsevier, 2015. 428 p.

[3] *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. 2 (2). С. 28—32.

[4] *Chauhan D., Gupta I., Verma R.* Quasigroups and their applications in cryptography // Cryptologia. 2021. Vol. 45, no. 3. P. 227—265.

[5] *Shcherbacov V.* Elements of Quasigroup Theory and Applications. Chapman, Hall/CRC, 2017.

[6] *Denes J., Keedwell A.* Latin squares and their applications (2nd edition). Elsevier, 2015. 428 p.

[7] *Тужилин М. Э.* Латинские квадраты и их применение в криптографии // Прикладная дискретная математика. 2012. Т. 17, № 3. С. 47—52.

В качестве непосредственного приложения квазигрупп в области симметричной криптографии можно привести следующие механизмы, основанные на квазигрупповых операциях, предлагаемые к рассмотрению в статьях македонских авторов С. Марковски, Д. Глигороски, В. Димитровой, А. Милевой и т.д.:

- поточные шифры и хэш-функции, основанные на квазигрупповом умножении[8],
- кандидат на стандартизацию в качестве поточного шифра **Edon80**[9],
- кандидаты на стандартизацию в качестве хэш-функции **Edon-R**[10] и **NaSHA**[11],
- кандидаты на стандартизацию в качестве низкоресурсной хэш-функции и алгоритма шифрования с ассоциированными (присоединенными) данными (AEAD-алгоритм) **GAGE** и **InGAGE**[12],
- предложения Г. Теселеану[13] и И.В. Чередника[14] по использованию квазигрупповых операций в рамках (обобщенных) сетей Фейстеля.

Однако недостаточная изученность задач, лежащих в основании подобных предложений, иногда приводит к возможности довольно простого криптоанализа

---

[8] *Markovski S.*, *Gligoroski D.*, *Bakeva V.* Quasigroup String Processing: Part 1 // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tect. Sci. XX. 1999. P. 157—162; *Markovski S.* Quasigroup string processing and applications in cryptography // Proc. 1-st Inter. Conf. Mathematics and Informatics for industry. Vol. 1002. 2003. P. 14—16; *Markovski S.*, *Bakeva V.* Quasigroup string processing: Part 4 // Contributions, Section of Natural, Mathematical and Biotechnical Sciences. 2017. Vol. 27, no. 1/2; Hash functions based on large quasigroups / V. Snášel, A. Abraham, J. Dvorskỳ, P. Krömer, J. Platoš // Computational Science–ICCS 2009: 9th International Conference Baton Rouge, LA, USA, May 25-27, 2009 Proceedings, Part I 9. Springer. 2009. P. 521—529.

[9] *Gligoroski D.*, *Markovski S.*, *Knapskog S. J.* The stream cipher Edon80 // New stream cipher designs. Springer, 2008. P. 152—169.

[10] *Gligoroski D.*, *Markovski S.*, *Kocarev L.* Edon-R, An Infinite Family of Cryptographic Hash Functions // International Journal of Security and Networks. 2009. Vol. 8, no. 3. P. 293–300; Cryptographic hash function Edon-R' / D. Gligoroski, R. S. Ødegård, M. Mihova, S. J. Knapskog, A. Drápal, V. Klima, J. Amundse, M. El-Hadedy // 2009 Proceedings of the 1st International Workshop on Security and Communication Networks. IEEE. 2009. P. 1—9.

[11] NaSHA Cryptographic Hash Function / S. Markovski, A. Mileva, S. Samardziska, B. Jakimovski. Algorithm Specifications and Supporting Documentations; *Mileva A.*, *Markovski S.* Quasigroup String Transformations and Hash Function Design: A Case Study: The NaSHA Hash Function // International Conference on ICT Innovations. Springer. 2009. P. 367—376.

[12] GAGE and InGAGE / D. Gligoroski, M. El-Hadedy, H. Mihajloska, D. Otte // A Submission to the NIST Lightweight Cryptography Standardization Process. 2019; *Gligoroski D.* On the S-box in GAGE and InGAGE. 2019. `http://gageingage.org/upload/LWC2019NISTWorkshop.pdf`.

[13] *Teşeleanu G.* Quasigroups and substitution permutation networks: a failed experiment // Cryptologia. 2021. Vol. 45, no. 3. P. 266—281; *Teşeleanu G.* The Security of Quasigroups Based Substitution Permutation Networks // International Conference on Information Technology and Communications Security. Springer. 2022. P. 306—319; *Teşeleanu G.* Cryptographic symmetric structures based on quasigroups // Cryptologia. 2023. Vol. 47, no. 4. P. 365—392.

[14] *Чередник И. В.* Один подход к построению транзитивного множества блочных преобразований // Прикладная дискретная математика. 2017. Т. 38. С. 5—34; *Чередник И. В.* Об использовании бинарных операций при построении транзитивного множества блочных преобразований // Дискретная математика. 2019. Т. 31, № 3. С. 93—113; *Чередник И. В.* Об использовании бинарных операций при построении кратно транзитивного множества блочных преобразований // Дискретная математика. 2020. Т. 32, № 2. С. 85—111.

полученных решений (см. работы М. Войводы и И. Сламинковой[15], М. Хелла и Т. Йохансона[16], И. Николича и Д. Ховратовича[17], Ж. Ли и соавторов[18]).

Квазигруппы (а также более сложные алгебраические структуры, в основе которых лежат квазигруппы) и их приложения в теории кодирования исследовались в ряде работ за авторством С. Гонсалеса, Е. Коусело, В.Т. Маркова, А.А. Нечаева, А.В. Михалёва, А.В. Грибова и других. Так, в статье[19] исследуются k-рекурсивные коды (т.е. коды, для которых позиции в кодовых словах с номерами $i+k$ однозначно определяются по позициям $i, i+1, \ldots, i+k-1$ для $i = k+1, \ldots, n-k$, иначе говоря, $u_{i+k} = f(u_i, \ldots, u_{i+k-1})$), лежащие на границе Синглтона (МДР-коды). Подход, основанный на применении ортогональных латинских квадратов, позволяет получить в данном случае оценки на максимальную длину кодовых слов. В серии работ[20] используются так называемые луповые кольца (формальные суммы квазигрупповых элементов) для построения различных оптимальных в разных смыслах кодов.

Луповые кольца и другие алгебраические структуры, основанные на квазигруппах, могут быть использованы для построения множества асимметричных криптографических примитивов. Такие конструкции исследовались С.Ю. Катышевым, В.Т. Марковым, А.А. Нечаевым, А.В. Михалёвым, А.В. Барышниковым, А.В. Грибовым, А.В. Зязиным, Е.С. Кислициным и другими авторами. В качестве примера можно привести следующие криптографические схемы и протоколы:

– протоколы формирования общего ключа — аналоги протокола Диффи-Хеллмана[21];

---

[15] *Vojvoda M.* Cryptanalysis of one hash function based on quasigroup // Tatra Mt. Math. Publ. 2004. Vol. 29, no. 3. P. 173—181; *Vojvoda M., Sýs M., Jókay M.* A note on algebraic properties of quasigroups in edon80 // Workshop Record of SASC. 2007; *Slaminková I., Vojvoda M.* Cryptanalysis of a hash function based on isotopy of quasigroups // Tatra Mountains Mathematical Publications. 2010. Vol. 45, no. 1. P. 137—149.

[16] *Hell M., Johansson T.* A key recovery attack on Edon80 // International Conference on the Theory and Application of Cryptology and Information Security. Springer. 2007. P. 568—581.

[17] *Nikolic I., Khovratovich D.* Free-start attacks on NaSHA. `https://ehash.isec.tugraz.at/uploads/3/33/Free-start_attacks_on_Nasha.pdf`.

[18] *Li Z., Jiang H., Li C.* Collision attack on NaSHA-384/512 // 2010 International Conference on Networking and Information Technology. IEEE. 2010. P. 243—246.

[19] Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы / С. Гонсалес, Е. Коусело, В. Т. Марков, А. А. Нечаев // Дискретная математика. 1998. Т. 10, № 2. С. 3—29.

[20] Групповые коды и их неассоциативные обобщения / С. Гонсалес, Е. Коусело, В. Т. Марков, А. А. Нечаев // Дискретная математика. 2004. Т. 16, № 1. С. 146—156; Loop codes / E. Couselo, S. González, V. T. Markov, A. A. Nechaev // Discrete Mathematics and Applications. 2004. Vol. 14, no. 2. P. 163—172; Квазигруппы и кольца в кодировании и построении криптосхем / В. Т. Марков, А. В. Михалёв, А. В. Грибов, П. А. Золотых, С. С. Скаженик // Прикладная дискретная математика. 2012. Т. 4; *Markov V. T., Mikhalev A. V., Nechaev A. A.* Nonassociative Algebraic Structures in Cryptography and Coding // Journal of Mathematical Sciences. 2020. Vol. 245, no. 2.

[21] *Катышев С. Ю., Марков В. Т., Нечаев А. А.* Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей // Дискретная математика. 2014. Т. 26, № 3. С. 45—64; *Марков В. Т., Михалёв А. В., Нечаев А. А.* Неассоциативные алгебраические структуры в криптографии и кодировании // Фундаментальная и прикладная математика. 2016. Т. 21, № 4.

– схемы асимметричного шифрования[22];
– схемы гомоморфного шифрования[23].

Отдельно можно выделить ряд работ, в которых изучаются схемы асимметричного шифрования и цифровой подписи, основанные на сложности решений систем уравнений в конечных полях (см. работы Д. Глигороски, С. Марковски, С. Кнапского, Й. Ченя и других[24]).

При этом применяемые в области защиты информации квазигруппы часто имеют довольно большие размеры (см., например, требования к квазигруппе в работах Д. Глигороски и соавторов[25]), что делает затруднительным поэлементное хранение в памяти компьютера всей таблицы умножения. Так, например, для построения хэш-функции Edon-$\mathcal{R}'$ необходимо задать квазигруппу порядка 2^{256}. В связи с этим обстоятельством в большинстве предлагаемых криптосистем большая квазигруппа строится, как правило, согласно одному из следующих подходов:

С. 99—124; *Baryshnikov A. V., Katyshev S. Y.* Key agreement schemes based on linear groupoids // Математические вопросы криптографии. 2017. Т. 8, № 1. С. 7—12; *Барышников А. В., Катышев С. Ю.* Использование неассоциативных структур для построения алгоритмов открытого распределения ключей // Математические вопросы криптографии. 2018. Т. 9, № 4. С. 5—30.

[22]Квазигруппы и кольца в кодировании и построении криптосхем / В. Т. Марков, А. В. Михалёв, А. В. Грибов, П. А. Золотых, С. С. Скаженик // Прикладная дискретная математика. 2012. Т. 4; *Грибов А. В., Золотых П. А., Михалёв А. В.* Построение алгебраической криптосистемы над квазигрупповым кольцом // Математические вопросы криптографии. 2010. Т. 1, № 4. С. 23—32; *Грибов А. В.* Алгебраические неассоциативные структуры и их приложения в криптографии : дис. … канд. / Грибов А. В. Московский государственный университет им. М. В. Ломоносова, 2015.

[23]*Грибов А. В.* Алгебраические неассоциативные структуры и их приложения в криптографии : дис. … канд. / Грибов А. В. Московский государственный университет им. М. В. Ломоносова, 2015; *Грибов А. В.* Гомоморфность некоторых криптографических систем на основе неассоциативных структур // Фундаментальная и прикладная математика. 2015. Т. 20, № 1. С. 135—143; *Katyshev S. Y., Zyazin A. V., Baryshnikov A. V.* Application of non-associative structures for construction of homomorphic cryptosystems // Математические вопросы криптографии. 2020. Т. 11, № 3. С. 31—39; *Марков В. Т., Михалёв А. В., Кислицын Е. С.* Неассоциативные структуры в гомоморфной криптографии // Фундаментальная и прикладная математика. 2020. Т. 23, № 2. С. 209—215.

[24]*Gligoroski D., Markovski S., Knapskog S. J.* A public key block cipher based on multivariate quadratic quasigroups // arXiv preprint arXiv:0808.0247. 2008; *Gligoroski D., Markovski S., Knapskog S. J.* Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups // Proceedings of the American Conference on Applied Mathematics. 2008. P. 44—49; *Chen Y., Knapskog S. J., Gligoroski D.* Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity // Submitted to ISIT. 2010. Vol. 2010. P. 14; MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme / D. Gligoroski, R. S. Ødegård, R. E. Jensen, L. Perret, J.-C. Faugere, S. J. Knapskog, S. Markovski // International Conference on Trusted Systems. Springer. 2011. P. 184—203.

[25]*Gligoroski D., Markovski S., Kocarev L.* Edon-R, An Infinite Family of Cryptographic Hash Functions // International Journal of Security and Networks. 2009. Vol. 8, no. 3. P. 293—300; Cryptographic hash function Edon-R' / D. Gligoroski, R. S. Ødegård, M. Mihova, S. J. Knapskog, A. Drápal, V. Klima, J. Amundse, M. El-Hadedy // 2009 Proceedings of the 1st International Workshop on Security and Communication Networks. IEEE. 2009. P. 1—9; *Chen Y., Knapskog S. J., Gligoroski D.* Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity // Submitted to ISIT. 2010. Vol. 2010. P. 14.

– случайная генерация квазигруппы (случайных поиск подходящей квазигруппы совместно с процедурой отсева неподходящих) из некоторого узкого класса (Д. Глигороски и соавторы[26]);
– итеративное построение большой квазигруппы из квазигрупп меньшего размера (Д. Глигороски и соавторы[27], А.В. Грибов[28]) с помощью конструкций произведений;
– изотопы некоторых «хорошо изученных» групп: например, изотоп группы точек эллиптической кривой (В.Т. Марков, А.В. Михалёв, А.А. Нечаев[29]), модульное вычитание (В. Снашель и соавторы[30]);
– функциональное задание квазигруппы, рассматриваемое в настоящей работе более подробно.

В работах В.А. Носова[31] был предложен метод задания латинского квадрата при помощи семейства булевых функций, которое определяет элемент квадрата по его координатам (номеру строки и столбца). Такие семейства функций, задающие целые параметрические классы латинских квадратов, были названы правильными. Понятие правильного семейства функций было сначала обобщено на случай абелевых групп (см. работы В.А. Носова, А.Е. Панкратьева, А.А. Козлова[32]), а затем и на более общие алгебраические структуры (см. работы

[26] *Gligoroski D., Markovski S., Knapskog S. J.* A public key block cipher based on multivariate quadratic quasigroups // arXiv preprint arXiv:0808.0247. 2008; *Chen Y., Knapskog S. J., Gligoroski D.* Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity // Submitted to ISIT. 2010. Vol. 2010. P. 14.

[27] Cryptographic hash function Edon-R' / D. Gligoroski, R. S. Ødegård, M. Mihova, S. J. Knapskog, A. Drápal, V. Klima, J. Amundse, M. El-Hadedy // 2009 Proceedings of the 1st International Workshop on Security and Communication Networks. IEEE. 2009. P. 1—9.

[28] *Грибов А. В.* Алгебраические неассоциативные структуры и их приложения в криптографии : дис. … канд. / Грибов А. В. Московский государственный университет им. М. В. Ломоносова, 2015.

[29] *Марков В. Т., Михалёв А. В., Нечаев А. А.* Неассоциативные алгебраические структуры в криптографии и кодировании // Фундаментальная и прикладная математика. 2016. Т. 21, № 4. С. 99—124.

[30] Hash functions based on large quasigroups / V. Snášel, A. Abraham, J. Dvorskỳ, P. Krömer, J. Platoš // Computational Science–ICCS 2009: 9th International Conference Baton Rouge, LA, USA, May 25-27, 2009 Proceedings, Part I 9. Springer. 2009. P. 521—529.

[31] *Носов В. А.* Критерий регулярности булевского неавтономного автомата с разделенным входом // Интеллектуальные системы. Теория и приложения. 1998. Т. 3, № 3/4. С. 269—280; *Носов В. А.* Построение классов латинских квадратов в булевой базе данных // Интеллектуальные системы. Теория и приложения. М., 1999. Т. 4, № 3/4. С. 307—320.

[32] *Носов В. А.* Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллектуальные системы. Теория и приложения. М., 2006. Т. 8, № 1—4. С. 517—529; *Носов В. А., Панкратьев А. Е.* Латинские квадраты над абелевыми группами // Фундаментальная и прикладная математика. 2006. Т. 12, № 3. С. 65—71; *Носов В. А., Панкратьев А. Е.* О семействах функций, задающих латинские квадраты над абелевыми группами // Лесной вестник Forestry bulletin. 2007. № 2; *Носов В. А., Панкратьев А. Е.* О функциональном задании латинских квадратов // Интеллектуальные системы. Теория и приложения. М., 2008. Т. 12, № 1—4. С. 317—332; *Козлов А. А., Носов В. А., Панкратьев А. Е.* Матрицы и графы существенной зависимости правильных семейств функций // Фундаментальная и прикладная математика. 2008. Т. 14, № 4. С. 137—149.

И.А. Плаксиной[33] и А.В. Галатенко, В.А. Носова, А.Е. Панкратьева[34]). Ряд работ посвящен изучению свойств введенных булевых отображений:

- В.А. Носовым[35] было (среди прочего) показано, что проверка свойства правильности является coNP-полной задачей (т.е. в общем случае задача проверки правильности является сложной),
- в работах В.А. Носова, А.Е. Панкратьева, А.А. Козлова[36] рассматривались свойства т.н. графа существенной зависимости правильных семейств (граф на n вершинах, ребро $i \to j$ присутствует в графе тогда и только тогда, когда j-я функция семейства зависит существенно от x_i) и были выделены широкие классы семейств, для которых свойство правильности эквивалентно свойству отсутствия циклов в графе существенной зависимости,
- в работах Д.О. Рыкова[37] показано, как задача проверки свойства правильности может быть упрощена, если дополнительно известна структура графа существенной зависимости семейства,
- работы И.А. Плаксиной[38] и А.В. Галатенко, В.А. Носова, А.Е. Панкратьева[39] посвящены, в том числе, различным способам задания (d-)квазигрупп с помощью правильных семейств над различными алгебраическими структурами,
- работы А.В. Галатенко, В.А. Носова, А.Е. Панкратьева, В.М. Староверова[40] посвящены вопросам построения новых правильных семейств функций из старых.

---

[33] *Плаксина И. А.* Построение параметрического семейства многомерных латинских квадратов // Интеллектуальные системы. Теория и приложения. 2014. Т. 18, № 2. С. 323–330.

[34] *Galatenko A. V., Nosov V. A., Pankratiev A. E.* Latin squares over quasigroups // Lobachevskii Journal of Mathematics. 2020. Vol. 41, no. 2. P. 194–203.

[35] *Носов В. А.* Критерий регулярности булевского неавтономного автомата с разделенным входом // Интеллектуальные системы. Теория и приложения. 1998. Т. 3, № 3/4. С. 269—280.

[36] *Носов В. А., Панкратьев А. Е.* О семействах функций, задающих латинские квадраты над абелевыми группами // Лесной вестник Forestry bulletin. 2007. № 2; *Носов В. А., Панкратьев А. Е.* О функциональном задании латинских квадратов // Интеллектуальные системы. Теория и приложения. М., 2008. Т. 12, № 1—4. С. 317—332; *Козлов А. А., Носов В. А., Панкратьев А. Е.* Матрицы и графы существенной зависимости правильных семейств функций // Фундаментальная и прикладная математика. 2008. Т. 14, № 4. С. 137—149.

[37] *Рыков Д. О.* Об алгоритмах проверки правильности семейств функций // Интеллектуальные системы. Теория и приложения. 2010. Т. 14, № 1—4. С. 261—276; *Рыков Д. О.* О правильных семействах функций, используемых для задания латинских квадратов // Интеллектуальные системы. Теория и приложения. 2014. Т. 18, № 1. С. 141—152.

[38] *Плаксина И. А.* Построение параметрического семейства многомерных латинских квадратов // Интеллектуальные системы. Теория и приложения. 2014. Т. 18, № 2. С. 323–330.

[39] *Galatenko A. V., Nosov V. A., Pankratiev A. E.* Latin squares over quasigroups // Lobachevskii Journal of Mathematics. 2020. Vol. 41, no. 2. P. 194–203.

[40] Порождение правильных семейств функций / А. В. Галатенко, В. А. Носов, А. Е. Панкратьев, В. М. Староверов // Интеллектуальные системы. Теория и приложения. 2021. Т. 25, № 4. С. 100—103; *Galatenko A. V., Pankratiev A. E., Staroverov V. M.* Generation of Proper Families of Functions // Lobachevskii Journal of Mathematics. 2022. Vol. 43, no. 3. P. 571–581.

При этом не всякая квазигруппа подходит для реализации на ее основе криптографических примитивов. Критически важными являются алгебраические свойства используемой квазигруппы, такие как свойства полиномиальной полноты (И. Хагеманн, К. Херрман[41]; Т. Нипков[42]; Г. Хорвац и соавторы[43]; В.А. Артамонов и соавторы[44]), количество ассоциативных троек (Т. Кепка[45]; А. Котзиг, К. Райшер[46]; Ж. Жезек, Т. Кепка[47]), наличие подквазигрупп (см., например, работу П.И. Собянина[48] и А.В. Галатенко, А.Е. Панкратьева, В.М. Староверова[49]). В ряде работ изучаются свойства квазигрупп, порождаемых правильными семействами булевых функций:

– Н.А. Пивнем[50] исследуются алгебраические свойства квазигрупп размера 4, порождаемых правильными семействами булевых функций размера $n = 2$, вводится понятие «перестановочной конструкции» (способ получения новых квазигрупп из уже имеющихся),
– в работе Н.А. Пивня[51] рассмотрена избыточность «перестановочной конструкции» (различные значения параметров могут давать одну и ту же квазигруппу) и способы сокращения избыточности,
– в работе А.В. Галатенко, В.А. Носова, А.Е. Панкратьева[52] предложен способ построения квадратичных квазигрупп, которые являются оптимальными с точки зрения криптографических приложений (обладают наиболее компактным представлением, при этом задача решения систем уравнений над подобными квазигруппами является в общем случае сложной),

---

[41] *Hagemann J., Herrmann C.* Arithmetical locally equational classes and representation of partial functions // Universal algebra. 1982. P. 345—360. Proceedings of the Colloquium on Universal Algebra.

[42] *Nipkow T.* Unification in primal algebras, their powers and their varieties // Journal of the ACM (JACM). 1990. Vol. 37, no. 4. P. 742—776.

[43] *Horváth G., Nehaniv C. L., Szabó C.* An assertion concerning functionally complete algebras and NP-completeness // Theoretical computer science. 2008. Vol. 407, no. 1—3. P. 591—595.

[44] *Artamonov V., Chakrabarti S., Pal S. k.* Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations // Discrete Applied Mathematics. 2016. Vol. 200. P. 5—17.

[45] *Kepka T.* A note on associative triples of elements in cancellation groupoids // Commentationes Mathematicae Universitatis Carolinae. 1980. Vol. 21, no. 3. P. 479—487.

[46] *Kotzig A., Reischer C.* Associativity index of finite quasigroups // Glasnik Matematicki Series III. 1983. Vol. 18, no. 38. P. 243—253.

[47] *Ježek J., Kepka T.* Notes on the number of associative triples // Acta Universitatis Carolinae. Mathematica et Physica. 1990. Vol. 31, no. 1. P. 15—19.

[48] *Собянин П. И.* Об алгоритме проверки наличия подквазигруппы в квазигруппе // Интеллектуальные системы. Теория и приложения. 2019. Т. 23, № 2. С. 79—84.

[49] *Галатенко А. В., Панкратьев А. Е., Староверов В. М.* Об одном алгоритме проверки существования подквазигрупп // Чебышевский сборник. 2021. Т. 22, 2 (78). С. 76—89.

[50] *Пивень Н. А.* Исследование квазигрупп, получаемых с помощью правильных семейств булевых функций порядка 2 // Интеллектуальные системы. Теория и приложения. 2018. Т. 22, № 1. С. 21—35.

[51] *Пивень Н. А.* Некоторые свойства перестановочной конструкции для параметрического задания квазигрупп // Интеллектуальные системы. Теория и приложения. 2019. Т. 23, № 2. С. 71—78.

[52] *Галатенко А. В., Носов В. А., Панкратьев А. Е.* Порождение квадратичных квазигрупп с помощью правильных семейств булевых функций // Фундаментальная и прикладная математика. 2020. Т. 23, № 2. С. 57—73.

– в дипломной работе А.С. Шварёва[53], среди прочего, рассмотрены «криптографические» свойств квазигрупп, порождаемых правильными семействами (линейная, дифференциальная характеристики) и способы их «усиления».

В контексте проведенных исследований остаются актуальными ряд нерешенных задач, исследованию которых и посвящена настоящая работа:

– изучение правильных семейств и их свойств как одного из возможных способов функционального задания квазигрупповой операции,
– изучение свойств квазигрупп, порождаемых правильными семействами.

Целью исследования является изучение свойств правильных семейств функций, а также алгебраических свойств квазигрупп, заданных правильными семействами функций. Тема, объект и предмет диссертационной работы соответствуют следующим пунктам паспорта специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика: теория алгебраических структур (полугрупп, групп, колец, полей, модулей и т.д.), теория дискретных функций и автоматов, теория графов и комбинаторика.

Для достижения поставленной цели автору необходимо было решить следующие **задачи**:

1. Получение новых критериев правильности семейств функций, а также установление естественного соответствия между правильными семействами функций и другими комбинаторно-алгебраическими структурами.
2. Исследование общих свойств правильных семейств функций, включая структуру множества неподвижных точек, а также стабилизатор относительно определенных классов преобразований.
3. Нахождение новых классов правильных семейств и изучение их свойств, включая мощность класса и мощность образа представителей.
4. Разработка нового способа построения квазигрупп на основе правильных семейств функций, создание шифра, сохраняющего формат, на основе этой конструкции, и анализ характеристик полученного шифра.

Научная новизна: результаты диссертации являются новыми и получены автором самостоятельно. Все результаты, выносимые автором на защиту, получены им лично. Результаты других авторов, используемые в диссертации, отмечены соответствующими ссылками. Основные результаты диссертации состоят в следующем.

1. Установлено естественное соответствие между булевыми правильными семействами и одностоковыми ориентациями графов булевых кубов (USO-ориентации), а также между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной

[53] *Шварёв А. С.* Криптоанализ и совершенствование квазигрупповых алгоритмов шифрования : дис. … маг. / Шварёв А. С. МГУ имени М.В. Ломоносова, Казахстанский филиал, 2024. выпускная квалификационная (бакалаврская) работа.

точкой (HUFP-сети); установлено естественное соответствие между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера.

2. Доказано, что стабилизатором множества правильных семейств функций являются изометрии пространства Хэмминга (согласованные перенумерации и перекодировки); показано, что отображения, задаваемые с помощью правильных семейств булевых функций, всегда имеют четное число неподвижных точек; получена оценка на число правильных семейств булевых функций, предложены оценки доли треугольных семейств среди всех правильных семейств булевых функций.
3. Построены новые классы правильных семейств функций (рекурсивно треугольные, локально треугольные, сильно квадратичное семейство); получены оценки на число рекурсивно треугольных семейств; для некоторых правильных семейств булевых функций получены точные значения мощности образа отображений, задаваемых этими правильными семействами.
4. Предложен новый способ порождения квазигрупп на основе правильных семейств функций; доказан ряд утверждений о числе ассоциативных троек в порождаемых квазигруппах; предложен новый алгоритм шифрования, сохраняющего формат (FPE-схема), основанный на квазигрупповых операциях.

Методология и методы исследования. В работе используются методы алгебры, дискретной математики, криптографии, теории графов, теории сложности.

Основные положения, выносимые на защиту:

1. Между булевыми правильными семействами и одностоковыми ориентациями графов булевых кубов (USO-ориентациями), а также между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной точкой (HUFP-сетями) существует естественное соответствие. Между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера также существует естественное соответствие.
2. Стабилизатор множества правильных семейств функций представляет собой множество пар согласованных изометрий пространства Хэмминга (согласованных перенумераций и перекодировок).
3. Отображения, задаваемые правильными семействами булевых функций, всегда имеют четное число неподвижных точек.
4. Мощность множества правильных семейств булевых функций размера n $T(n)$ удовлетворяет отношению $\log_2(T(n)) = \Theta(2^n \cdot \log_2(n))$. Треугольные семейства составляют бесконечно малую долю среди всех правильных семейств булевых функций.
5. Локально треугольные, рекурсивно треугольные и сильно квадратичное семейства являются правильными. Мощность образов рассмотренных

в работе квадратичных булевых правильных семейств близка к максимально возможной.

6. Предложенная в работе конструкция позволяет порождать квазигруппы с помощью правильных семейств функций. Алгоритм шифрования, построенный на основе этой конструкции, сохраняет формат исходных сообщений (является FPE-схемой). Ряд утверждений о числе ассоциативных троек в квазигруппах, построенных на основе предложенной конструкции, позволяет свести вопрос об изучении индексов ассоциативности от всех пар правильных семейств к классам эквивалентности пар правильных семейств.

Достоверность полученных результатов обеспечивается строгими математическими доказательствами. Результаты работы докладывались на научных конференциях, опубликованы в рецензируемых научных журналах и находятся в соответствии с результатами, полученными другими авторами. Результаты других авторов, используемые в диссертации, отмечены соответствующими ссылками.

Апробация работы. Основные результаты работы докладывались на следующих международных и всероссийских конференциях:

1. XXVI Международная конференция студентов, аспирантов и молодых учёных «Ломоносов», Москва, Россия, с 8 по 12 апреля 2019 г.;
2. X симпозиум «Современные тенденции в криптографии» (CTCrypt 2021), Дорохово, Россия, с 1 по 4 июня 2021 г.;
3. XI симпозиум «Современные тенденции в криптографии» (CTCrypt 2022), Новосибирск, Россия, с 6 по 9 июня 2022 г.;
4. Четырнадцатый международный семинар «Дискретная математика и ее приложения» имени академика О.Б. Лупанова под руководством В. В. Кочергина, Э. Э. Гасанова, С. А. Ложкина, А. В. Чашкина, с 20 по 25 июня 2022 г.;
5. 11-я Международная конференция «Дискретные модели в теории управляющих систем», Красновидово, Россия, с 26 по 29 мая 2023 г.;
6. Третья Международная конференция “MATHEMATICS IN ARMENIA: ADVANCES AND PERSPECTIVES”, Ереван, Армения, со 2 по 8 июля 2023 г.;
7. 22-я Международная конференция «Сибирская научная школа-семинар “Компьютерная безопасность и криптография” имени Геннадия Петровича Агибалова», Барнаул, Россия, с 4 по 9 сентября 2023 г.;
8. Международная конференция «Математика в созвездии наук», Москва, Россия, с 1 по 2 апреля 2024 г.;
9. Международная конференция «Алгебра и математическая логика: теория и приложения», Казань, Россия, с 27 июня по 1 июля 2024 г.;
10. XX Международная научная конференция «Проблемы теоретической кибернетики», Москва, Россия, с 5 по 8 декабря 2024 г.

Результаты работы докладывались и обсуждались на заседаниях следующих научных семинаров:

1. научно-исследовательский семинар по алгебре механико-математического факультета МГУ под руководством Д. О. Орлова, М. В. Зайцева, 2023 г.;
2. научно-исследовательский семинар «Математические вопросы кибернетики» кафедр дискретной математики и математической теории интеллектуальных систем механико-математического факультета и математической кибернетики факультета вычислительной математики и кибернетики МГУ под руководством Э. Э. Гасанова, В. В. Кочергина, С. А. Ложкина, 2023 г.;
3. семинар «Компьютерная алгебра» факультета ВМК МГУ и ВЦ РАН под руководством профессора С. А. Абрамова, 2023 г.;
4. семинар «Теория автоматов» механико-математического факультета МГУ под руководством профессора Э. Э. Гасанова, 2023 г.;
5. семинар «Современные проблемы криптографии» под руководством ведущего научного сотрудника В. А. Носова и доцента А. Е. Панкратьева, механико-математический факультет МГУ, неоднократно;
6. семинар «Компьютерная безопасность» под руководством старшего научного сотрудника А.В. Галатенко, механико-математический факультет МГУ, неоднократно.

Публикации. Основные результаты по теме диссертации изложены в 9 печатных изданиях, 8 из которых опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика, из них 6 — в рецензируемых научных изданиях, входящих в ядро РИНЦ и международные базы цитирования (Web of Science / Scopus), RSCI, 2 — в рецензируемых научных изданиях из дополнительного списка МГУ, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика и входящих в список ВАК.

Структура работы. Диссертация состоит из введения, 4 глав и заключения. Полный объём диссертации составляет 143 страницы, включая 5 рисунков и 9 таблиц. Список литературы содержит 171 наименование.

Содержание работы

Во **Введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель, ставятся задачи исследования, излагается научная новизна и практическая значимость представляемой работы.

Первая глава посвящена введению основных определений, используемых далее на протяжении всей работы. Вводится понятие d-квазигруппы —

множества Q с заданной на нем операцией $h\colon Q^d \to Q$ со свойством однозначной разрешимости уравнения $h(x_1, \ldots, x_d) = y$ при фиксации любых d значений переменных $\{x_1, \ldots, x_d, y\}$ относительно свободной переменной. При $d = 2$ операция h часто обозначается через $\circ$ и записывается в инфиксной нотации ($x \circ y = z$). Также рассматривается понятие семейства отображений $\mathcal{F}\colon Q^n \to Q^n$ на Q^n, где $\mathcal{F} = (f_1, \ldots, f_n)$, $f_i\colon Q^n \to Q$,

$$\mathcal{F}(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)),$$

обсуждаются некоторые свойства таких семейств и их возможные преобразования: внешние и внутренние сдвиги, согласованные перестановки, сужения. Вводится понятие проекции семейства $\mathcal{G}_{n-1} = \Pi_i^q(\mathcal{F}_n)$, где $q \in Q$, получаемого из $\mathcal{F}_n$ подстановкой вместо переменной x_i константы q и вычеркиванием функции f_i.

Если $Q = \mathbb{E}_2 = \{0, 1\}$, то семейство $\mathcal{F}$ на $Q^n = \mathbb{E}_2^n$ называется семейством булевых функций. Для семейства булевых функций $\mathcal{F}_n = (f_1, \ldots, f_n)$ вводится понятие строгой квадратичности: $\mathcal{F}_n$ называется квадратичным семейством строгого типа $Quad_v^s Lin_{n-v}^s$, $1 \le v \le n$, если

- каждая функция семейства не более чем квадратична,
- имеется v функций, все нетривиальные линейные комбинации которых квадратичны,
- если $v < n$, то для любых $v+1$ функций найдется нетривиальная линейная комбинация, степень которой меньше двух.

Если $v = n$, то семейство $\mathcal{F}_n$ называется сильно квадратичным.

Далее вводится основной объект исследования — правильное семейство функций. Семейство $\mathcal{F}\colon Q^n \to Q^n$ называется правильным, если для любых неравных наборов $\alpha, \beta \in Q^n$ найдется такой индекс $1 \le i \le n$, что $\alpha_i \ne \beta_i$, но $f_i(\alpha) = f_i(\beta)$. Рассматриваются некоторые свойства правильных семейств (булевых) функций. В частности, доказана следующая теорема (теорема 1), являющаяся обобщением критерия регулярности (утверждение 4): семейство $\mathcal{F}_n$ на Q^n является правильным тогда и только тогда, когда для любого набора отображений $\psi_i\colon Q \to Q$, $1 \le i \le n$, следующее отображение из Q^n в себя биективно:

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to \mathbf{x} \circ \Psi(\mathcal{F}_n(\mathbf{x})) = \begin{bmatrix} x_1 \circ \psi_1(f_1(x_1, \ldots, x_n)) \\ \vdots \\ x_n \circ \psi_n(f_n(x_1, \ldots, x_n)) \end{bmatrix}, \; x_i \in Q_i.$$

Рассматриваются различные примеры правильных семейств: константные, треугольные, линейные и ортогональные семейства, треугольные расширения.

Отдельно рассматриваются два семейства специального вида. Доказано, что семейства

$$\begin{bmatrix} 0 \\ x_1 \\ x_1 \oplus x_2 \\ \vdots \\ x_1 \oplus x_2 \oplus \ldots \oplus x_{n-1} \end{bmatrix} \bigoplus \begin{bmatrix} \bigoplus_{i<j,\ i,j\neq 1}^{n} x_i x_j \\ \bigoplus_{i<j,\ i,j\neq 2}^{n} x_i x_j \\ \bigoplus_{i<j,\ i,j\neq 3}^{n} x_i x_j \\ \vdots \\ \bigoplus_{i<j,\ i,j\neq n}^{n} x_i x_j \end{bmatrix}$$

являются правильными для любого $n \geq 1$ (теорема 2), семейства

$$\mathcal{F}(\mathbf{x}) = \begin{bmatrix} f_1(x_1, \ldots, x_n) \\ f_2(x_1, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_n) \end{bmatrix} = \begin{bmatrix} \overline{x}_2 \cdot x_3 \\ \overline{x}_3 \cdot x_4 \\ \vdots \\ \overline{x}_1 \cdot x_2 \end{bmatrix}$$

при $n \geq 3$ являются квадратичными строгого типа $Quad^s_{n-1}Lin^s_1$ при четных n и квадратичными строгого типа $Quad^s_n Lin^s_0$ (сильно квадратичными) при нечетных n (теорема 3).

Далее рассматриваются основные свойства квазигрупп, релевантные с точки зрения криптографических приложений: полиномиальная полнота, отсутствие подквазигрупп, количество ассоциативных троек. Доказывается ряд утверждений о числе ассоциативных троек в квазигруппах, задаваемых операцией

$$\mathbf{x} \circ \mathbf{y} = \mathbf{x} + \mathcal{F}(\mathbf{x}) + \mathbf{y} + \mathcal{G}(\mathbf{y}),\ \mathbf{x}, \mathbf{y} \in G^n,$$

где $(G, +)$ — группа (необязательно коммутативная), $\mathcal{F}, \mathcal{G}$ — правильные семейства на G^n. В частности, показано, что тройка $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ является ассоциативной в квазигруппе $(G^n, \circ)$, построенной по паре семейств $(\mathcal{F}, \mathcal{G})$, тогда и только тогда, когда тройка $(\mathbf{z}, \mathbf{y}, \mathbf{x})$ является ассоциативной в квазигруппе, построенной по паре семейств $(\mathcal{G}, \mathcal{F})$ (теорема 5). Для булева случая $(G, +) = (\mathbb{Z}_2, \oplus)$ показана справедливость двух дополнительных утверждений:

- тройка $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ является ассоциативной для квазигруппы, построенной по паре правильных булевых семейств $(\mathcal{F}, \mathcal{G})$, тогда и только тогда, когда она является ассоциативной для квазигруппы, построенной по паре правильных булевых семейств $(\mathcal{F} \oplus \alpha, \mathcal{G} \oplus \alpha)$, где $\alpha \in \mathbb{Z}_2^n$ (теорема 7);
- количество ассоциативных троек в квазигруппе, построенной по паре правильных булевых семейств $(\mathcal{F}, \mathcal{G})$, четно (теорема 8).

Результаты главы были опубликованы в [1—3; 7].

Во **второй главе** рассматриваются эквивалентные определения правильности. Вводятся понятия одностоковой ориентации булева куба (USO-ориентации), асинхронной булевой сети с наследственно неподвижной общей точкой (HUFP-сети), графа семейства $\Gamma_{\mathcal{F}}$. Показано, что у правильного семейства булевых функций как отображения $\mathbb{E}_2^n \to \mathbb{E}_2^n$ всегда существует единственная неподвижная точка (лемма 1), с помощью этого утверждения устанавливается два характеристических свойства булевых правильных семейств:

– граф семейства $\Gamma_{\mathcal{F}}$ является одностоковой ориентацией булева куба $\mathbb{E}_n$ тогда и только тогда, когда $\mathcal{F}$ — правильное семейство (теорема 9);
– существует естественное соответствие между правильными булевыми семействами и HUFP-сетями (теорема 12).

Полученные соответствия позволяют получить ряд следствий, переведя часть результатов из области USO-ориентаций и HUFP-сетей на «язык» правильных семейств функций.

Так, получено ограничение $\log_2(T(n)) = \Theta(2^n \cdot log_2(n))$ на порядок роста числа правильных семейств булевых функций $T(n)$ размера n при $n \to \infty$ (утверждение 23). Для булевых треугольных семейств с помощью установленного выше факта удается показать, что их количество $\Delta(n)$ есть о-малое от общего числа всех правильных булевых семейств:

$$\frac{\Delta(n)}{T(n)} = o\left(\frac{1}{n^{D \cdot 2^n}}\right) \text{ при } n \to \infty$$

для некоторого $D > 0$ (теорема 10).

Соответствие между USO-ориентациями, HUFP-сетями и правильными семействами позволяет получать новые примеры классов правильных семейств функций. Семейство $\mathcal{F}\colon Q^n \to Q^n$ назовем

– рекурсивно треугольным, если существует такая координата i, что $f_i = q \in Q$ (константа), и каждое из семейств вида $\Pi_i^a(\mathcal{F})$, где a пробегают все множество Q, также является рекурсивно треугольным.
– локально треугольным, если для каждой точки $\mathbf{x} \in Q^n$ существует такая согласованная перестановка семейства σ, что после ее применения мы получим семейство $\mathcal{G}$ со свойством

$$\partial_i g_j(\mathbf{x}) = 0, \quad 1 \le j \le i \le n,$$

где $\partial_i(f)$ — частная производная функции f по направлению i.

Доказан ряд утверждений о введенных классах семейств.

1. Локально треугольные семейства являются правильными (теорема 13).
2. Класс рекурсивно треугольных семейств вкладывается в класс локально треугольных семейств; в частности, все рекурсивно треугольные семейства являются правильными (лемма 9).
3. Для числа рекурсивно треугольных семейств получена формула

$$\Delta_k^{\mathsf{rec}}(n) = \sum_{j=1}^{n} (-1)^{j+1} \cdot k^j \cdot \binom{n}{j} \left(\Delta_k^{\mathsf{rec}}(n-j)\right)^{k^j},$$

где $\Delta_k^{\mathsf{rec}}(0) = 1$, $k = |Q|$ (лемма 5).
4. Доля булевых рекурсивно треугольных семейств размера n в классе всех булевых правильных семейств размера n стремится к 0 при $n \to \infty$ (теорема 11).

Также в главе рассматривается кликовое задание правильных семейств. Зададим обобщенный граф Келлера $G(k,n)$ следующим образом:

– множество вершин графа V — наборы чисел от 0 до k^2-1 длины n: $V=\mathbb{E}_{k^2}^n$,
– пара $\{v,w\}$ принадлежит множеству ребер E тогда и только тогда, когда найдется координата i, $1\le i\le n$, что выполнены два условия:

$$v_i \equiv w_i \bmod k,\ v_i \neq w_i.$$

Показано, что правильные семейства $\mathcal{F}_n$ на $\mathbb{E}_k^n$ находятся во взаимнооднозначном соответствии с **кликами** в графе $G(k,n)$ размера k^n: по правильному семейству строится клика в графе $G(k,n)$, и наоборот, по каждой клике размера k^n в $G(k,n)$ задается правильное семейство на $\mathbb{E}_k^n$ (теорема 14).

В конце главы рассматривается некоторое расширение понятия правильности на основе свойства неортогональности аффинных подпространств. Вводится понятие обобщенно правильного семейства в k-значной логике, показывается, что при $k=2$ введенное понятие совпадает со стандартным понятием правильного семейства. Доказывается, что понятие обобщенной правильности может быть задано эквивалентным образом через понятие неортогональности (теоремы 15, 16).

Результаты главы ранее были опубликованы в [1; 4; 8].

Третья глава посвящена исследованию некоторых свойств правильных семейств. Решена задача о поиске стабилизатора множества правильных семейств относительно действия

$$\mathcal{G}=(\Phi,\Psi)\curvearrowright\mathcal{F},\ \mathcal{G}(\mathbf{x})\to\Phi(\mathcal{F}(\Psi(\mathbf{x}))),$$

где $\Phi,\Psi\in\mathcal{S}_{\mathbb{E}_k^n}$ — биекции. Фактически, показано, что стабилизаторами множества правильных семейств являются «согласованные» изометрии пространства Хэмминга (теорема 18).

Доказан ряд результатов для булевых правильных семейств $\mathcal{F}_n$:

– для любого $\alpha\in\mathbb{E}_2^n$ число решений уравнения $\mathcal{F}_n(\mathbf{x})=\alpha$ всегда четно (теорема 19),
– для отображения, задаваемого семейством

$$\begin{bmatrix} 0 \\ x_1 \\ x_1\oplus x_2 \\ \vdots \\ x_1\oplus x_2\oplus\ldots\oplus x_{n-1}\end{bmatrix}\bigoplus\begin{bmatrix}\bigoplus_{i<j,\ i,j\neq 1}^n x_ix_j \\ \bigoplus_{i<j,\ i,j\neq 2}^n x_ix_j \\ \bigoplus_{i<j,\ i,j\neq 3}^n x_ix_j \\ \vdots \\ \bigoplus_{i<j,\ i,j\neq n}^n x_ix_j\end{bmatrix},$$

мощность образа максимальна (в классе отображений, задаваемых правильными булевыми семействами) и равна 2^{n-1}, т.е. семейство имеет максимально возможную мощность образа (теорема 20),

– для отображения, задаваемого семейством

$$\mathcal{F}(\mathbf{x}) = \begin{bmatrix} f_1(x_1, \ldots, x_n) \\ f_2(x_1, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_n) \end{bmatrix} = \begin{bmatrix} \overline{x}_2 \cdot x_3 \\ \overline{x}_3 \cdot x_4 \\ \vdots \\ \overline{x}_1 \cdot x_2 \end{bmatrix}$$

мощность образа равна Lucas_n, n-му числу Люка (теорема 21).

Также изучаются некоторые алгебраические свойства отображений, порождаемых правильными семействами функций. Будем через $\mathcal{S}^{\mathsf{prop}}$ обозначать множество таких подстановок $\sigma \in \mathcal{S}_{Q^n}$, что отображение $\mathcal{F}_n$ вида

$$\mathcal{F}_n(\mathbf{x}) = L_{\mathbf{x}}^{-1}\left(\sigma(\mathbf{x})\right) = \begin{bmatrix} L_{x_1}^{-1}(\sigma_1(\mathbf{x})) \\ \vdots \\ L_{x_n}^{-1}(\sigma_n(\mathbf{x})) \end{bmatrix},$$

где $L_x(y) = x \circ y$, является правильным на Q^n. Пусть $\mathcal{F}$ — правильное семейство на G^n, $(G, \cdot)$ — группа, рассмотрим *дуальное* к семейству $\mathcal{F}$ семейство $\mathcal{G}$, соответствующее подстановке σ^{-1}:

$$\mathcal{G} \colon Q^n \to Q^n, \quad \mathcal{G}(\mathbf{x}) = \mathbf{x} \cdot \sigma^{-1}(\mathbf{x}).$$

– множество $\mathcal{S}^{\mathsf{prop}}$ замкнуто относительно взятия обратной подстановки: отображение $\mathcal{G}(\mathbf{x})$ является правильным на Q^n (теорема 22),
– замыкание $\langle \mathcal{S}^{\mathsf{prop}} \rangle$ действует транзитивно на множестве Q^n (теорема 24),
– для булева случая показано, что каждая подстановка $\pi \in \mathcal{S}^{\mathsf{prop}}$ всегда имеет четное число неподвижных точек (теорема 23).

Результаты главы ранее были опубликованы в [1; 2; 5].

В **четвертой главе** приведены результаты, касающиеся алгоритмических и вычислительных аспектов:

– предлагается к рассмотрению один алгоритм шифрования, сохраняющего формат (т.н. FPE-алгоритм), основанный на квазигрупповых сдвигах в квазигруппах, порожденных правильными семействами булевых функций,
– приводятся точные значение количества булевых правильных семейств в различных классах (треугольные, рекурсивно и локально треугольные семейства),
– рассматриваются результаты численных экспериментов по вычислению индексов ассоциативности квазигрупп, заданных с помощью правильных семейств, а также результаты вычислительных экспериментов для проверки свойств аффинности и простоты для квазигрупп, порожденных парами правильных семейств.

Результаты главы ранее были опубликованы в [7; 6; 9].

В **заключении** приведены основные результаты работы, которые состоят в следующем.

1. Установлено естественное соответствие между булевыми правильными семействами и одностоковыми ориентациями графов булевых кубов (USO-ориентации).
2. Установлено естественное соответствие между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной точкой (HUFP-сети).
3. Установлено естественное соответствие между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера.
4. Доказано, что стабилизатором множества правильных семейств функций являются изометрии пространства Хэмминга (согласованные перенумерации и перекодировки).
5. Показано, что отображения, задаваемые с помощью правильных семейств булевых функций, всегда имеют четное число неподвижных точек.
6. Получена оценка на число правильных семейств булевых функций, предложены оценки доли треугольных семейств среди всех правильных семейств булевых функций.
7. Обнаружены и исследованы новые классы правильных семейств функций (рекурсивно треугольные, локально треугольные, сильно квадратичное семейство).
8. Получены оценки на число рекурсивно треугольных семейств.
9. Для некоторых правильных семейств булевых функций получены точные значения мощности образа отображений, задаваемых этими правильными семействами.
10. Предложен новый способ порождения квазигрупп на основе правильных семейств функций.
11. Доказан ряд утверждений о числе ассоциативных троек в порождаемых квазигруппах.
12. Предложен новый алгоритм шифрования, сохраняющего формат (FPE-схема), основанный на квазигрупповых операциях.

Результаты диссертационной работы могут представлять интерес для специалистов, работающих в области теории дискретных и булевых функций, теории квазигрупп, криптографии.

В качестве тем для дальнейших исследований можно отметить следующие направления.

1. Предложить способ построения достаточно широких классов правильных семейств с хорошими алгебраическими и комбинаторными свойствами, в том числе и для логик большей значности $k > 2$.
2. Предложить способ быстрого построения множества представителей всех правильных семейств размера $n + 1$ с помощью представителей размера n и менее (с точностью до согласованных перенумераций и перекодировок).

3. Предложить альтернативные геометрические описания правильных семейств в k-значной логике, где $k > 2$, которые были бы инвариантны относительно согласованных перенумераций и перекодировок.
4. Предложить алгоритм, полиномиальный по длине входа, на вход принимающий правильное семейство (например, в виде КНФ или полиномов Жегалкина) и параметрические подстановки и выдающий количество ассоциативных троек (или нижние и верхние границы на число троек), проверяющий полиномиальную полноту порождаемой квазигруппы, наличие или отсутствие подквазигрупп.
5. Оценить генерическую сложность задачи решения системы уравнений над квазигруппами, заданными правильными семействами.

Публикации автора по теме диссертации

Научные статьи, опубликованные в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика и входящих в базы цитирования Scopus, Web of Science и RSCI

1. *Царегородцев К.* О свойствах правильных семейств булевых функций // Дискретная математика. — 2021. — Т. 33, № 1. — С. 91—102.
   EDN: JTVVAY; журнал индексируется в RSCI. Импакт-фактор: 0.385 (РИНЦ); общий объем 0.75 п. л.
   Перевод:
   Tsaregorodtsev K.D. Properties of proper families of Boolean functions // Discrete Mathematics and Applications. — 2022. — vol. 32, no. 5. — pp. 369–378.
   EDN: INXYMW; журнал индексируется в WOS, Scopus. Импакт-фактор: 0.3 (JIF); общий объем 0.75 п. л.
2. О порождении n-квазигрупп с помощью правильных семейств функций / А. Галатенко, В. Носов, А. Панкратьев, К. Царегородцев // Дискретная математика. — 2023. — Т. 35, № 1. — С. 35—53.
   EDN: WWYSEG; журнал индексируется в RSCI Импакт-фактор: 0.385 (РИНЦ); общий объем 1.18 п.л.
   Царегородцеву К. Д. принадлежат формулировка и доказательство теоремы 1 и результаты раздела 6, 29 %, объем 0.34 п. л.
   Перевод:
   Galatenko A.V., Nosov V.A., Pankratiev A.E., Tsaregorodtsev K.D. Generation of n-quasigroups by proper families of functions // Discrete Mathematics and Applications. — 2025. — vol. 35, no. 4. — pp. 203–217.
   DOI: https://doi.org/10.4213/dm1749, журнал индексируется в WOS, Scopus. Импакт-фактор: 0.3 (JIF); общий объем 1.18 п.л.
   Царегородцеву К. Д. принадлежат формулировка и доказательство теоремы 1 и результаты раздела 6, 29 %, объем 0.34 п. л.

3. Proper families of functions and their applications / A. V. Galatenko, V. A. Nosov, A. E. Pankratiev, K. D. Tsaregorodtsev // Математические вопросы криптографии. — 2023. — Т. 14, № 2. — С. 43—58.
   EDN: FUKEYM; журнал индексируется в RSCI. Импакт-фактор: 0.232 (РИНЦ); общий объем 0.98 п. л.
   Царегородцеву К. Д. принадлежат разделы 4,5,6, 25 %, объем 0.25 п. л.

4. *Царегородцев К. Д.* О взаимно однозначном соответствии между правильными семействами булевых функций и рёберными ориентациями булевых кубов // Прикладная дискретная математика. — 2020. — Т. 48. — С. 16—21.
   EDN: VTEBFJ; журнал индексируется в Scopus, RSCI. Импакт-фактор: 0.1 (JIF); общий объем 0.375 п. л.

5. *Galatenko A.*, *Pankratiev A.*, *Tsaregorodtsev K.* A Criterion of Properness for a Family of Functions // Journal of Mathematical Sciences. — 2024. — vol. 284, no. 4. — pp. 451—459.
   EDN: ECXXNP; журнал индексируется в Scopus. Импакт-фактор: 0.28 (SJR); общий объем 0.81 п. л.
   Царегородцеву К. Д. принадлежат формулировка и доказательство результатов раздела 4, 38 %, объем 0.31 п. л.

6. *Tsaregorodtsev K.* Format-preserving encryption: a survey // Математические вопросы криптографии. — 2022. — Т. 13, № 2. — С. 133—153.
   EDN: QMBWSF; журнал индексируется в RSCI. Импакт-фактор: 0.232 (РИНЦ); общий объем 1.31 п. л.

Публикации в рецензируемых научных изданиях из дополнительного списка МГУ, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика и входящих в список ВАК

7. *Царегородцев К.* Об индексе ассоциативности конечных квазигрупп // Интеллектуальные системы. Теория и приложения. — 2024. — Т. 28, № 3. — С. 80—101.
   Импакт-фактор: 0.117 (РИНЦ); 1.37 п. л.

8. *Царегородцев К.* О соответствии между правильными семействами и реберными ориентациями булевых кубов // Интеллектуальные системы. Теория и приложения. — 2020. — Т. 24, № 1. — С. 97—100.
   EDN: EYLHYQ. Импакт-фактор: 0.117 (РИНЦ); общий объем 0.25 п. л.

Публикации в прочих изданиях

9. *Царегородцев К.* Об одном квазигрупповом алгоритме шифрования, сохраняющего формат // Прикладная дискретная математика. Приложение. — 2023. — Т. 16. — С. 102—104.
   EDN: NOTNOY. Импакт-фактор: 0.056 (РИНЦ); 0.15 п. л.

Царегородцев Кирилл Денисович

Правильные семейства функций и
порождаемые ими квазигруппы:
комбинаторные и алгебраические свойства

Автореф. дис. на соискание ученой степени канд. физ.-мат. наук

Подписано в печать ___.___._____. Заказ № _____
Формат 60×90/16. Усл. печ. л. 1. Тираж 100 экз.
Типография _____